UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NORTH CAROLINA
WESTERN DIVISION

NO. 5:18-CR-00461-BO

UNITED STATES OF AMERICA	)	
	)	
v.	)	SENTENCING MEMORANDUM
	)	
SERGIY PETROVICH USATYUK	)	
	)	

The United States of America, by and through the United States Attorney for the Eastern District of North Carolina, and the Assistant Attorney General of the Criminal Division, respectfully submits the following sentencing memorandum.

I. Introduction

The defendant, Sergiy P. Usatyuk, made a lucrative business out of launching millions of cyber-attacks on behalf of thousands of cyber criminals. The attacks were widespread, indiscriminate, and victimized wide swaths of American society, including law enforcement, schools, military webpages (.MIL), government research labs, U.S. Department of Defense ("DoD") entities, large and small corporations, and residential communities. They continued unabated for 27 months. As a consequence of these attacks, school and governmental services were disrupted, targeted computer systems were knocked offline, the price of doing business online was increased, and organizations, such as the DoD, had to waste valuable resources combatting the serious threat posed by the defendant's attacks.

To profit from enabling cyber-crime on a massive scale, the defendant and a co-conspirator created criminal web-based services called "booters" that customers

could use to order illegal distributed denial of service ("DDoS") attacks, developed and managed supporting software and computer infrastructure, provided customer service, and contracted with third-parties for supporting services. To conceal his identity and criminal activity, the defendant also attempted to obscure the role of the co-conspirators' criminal infrastructure in launching DDoS attacks, used aliases and online monikers, deceived third-parties, created a vast network of payment processing accounts under fake identities to receive payments for illegal services, and channeled the illegal proceeds of their scheme through cryptocurrency.

The defendant did all of this knowing that his criminal services were launching millions of illegal cyber-attacks. Indeed, in emails and electronic chats, the defendant often acknowledged that booting services, like his, are illegal, and discussed plans to destroy evidence to avoid accountability. The defendant's fear of law enforcement action was not speculative. Notably, eighteen months before joining the charged conspiracy (March 2014), the FBI ***personally*** told the defendant that his cyber-attacks were illegal and must stop during two interviews concerning his role in an earlier large-scale attack that took down an influential technology website. Yet, the defendant ignored the warnings and dramatically escalated the seriousness and scope of his criminal conduct. The defendant's history therefore reflects a troubling combination of sophistication, recidivism, and disregard for the rule of law that makes him a serious threat to the American public if undeterred.

The United States Probation Office ("USPO") correctly calculated a guideline sentence that includes a term of incarceration of between 57 and 60 months. The

government respectfully submits that a sentence of **57** months is sufficient, but not greater than necessary, to reflect the seriousness of the crime and the significant harm caused by the defendant's services, as well as protect the American public from future crime and deter others who may seek to profit from widespread cyber-crime.

II. Offense Conduct

a. The Defendant Owned, Administered, and Supported the Criminal Subject Booter Services

Between approximately August 2, 2015 and November 30, 2017, the defendant conspired with another cyber-criminal (Co-Conspirator A) to unlawfully profit from the ownership, administration, and support of the criminal web-based booter services ExoStress.in ("ExoStresser"), QuezStresser.com ("QuezStresser"), Betabooter.com ("Betabooter"), Databooter.com ("Databooter"), Instabooter.com ("Instabooter"), Polystress.com ("Polystress"), Decafestresser, and Zstress.net ("Zstress") (collectively, "the Booters"). (PSR at ¶ 6). As part of the scheme, the defendant and Co-Conspirator A also administered and supported websites, such as Bestipstressers.com and Ipstressers.org (the "Promoter Websites"), that promoted the Subject Booters and advertised other booter services (collectively, the "Booter Services"). (*Id.*).

In furtherance of the scheme, the defendant and Co-Conspirator A controlled and operated public-facing websites for the Booters that cybercriminals used to order DDoS attacks and input related attack instructions against intended victim computer systems, including the victim's unique online identifiers, the attack length, the number of servers supporting the attack, and the type of attack. (PSR at ¶ 7). The defendant and Co-Conspirator A also developed and maintained source code for

processing and routing the Booters' attack orders through a network of servers that they controlled. (*Id.*) These servers, in turn, typically launched the Booters' DDoS attacks by spoofing the Internet Protocol ("IP") addresses of the intended victims in electronic messages to third-party, Internet-enabled devices (the "amplification servers") that were deceived into reflecting and amplifying junk traffic towards the intended victim without the knowledge and consent of the amplification servers' owners. (*Id.*). The co-conspirators also developed or obtained lists of amplification servers that would be exploited by the Booters' DDoS attacks. (DE-1 [Criminal Information] at ¶ 9).

The defendant and Co-Conspirator A generated huge profits from charging the Booters'[1] customers variable subscription fees that were tailored to the customer's specific DDoS attack instructions. (PSR at ¶ 7). To promote the Booters and generate additional revenue, the defendant and Co-Conspirator A also operated the Promoter Websites. (*Id.* ¶ 6). In total, the defendant personally made at least $542,925 from owning and operating the Subject Booter Services and supporting computer infrastructure, and the conspirators as a whole are conservatively estimated to have gained at least $557,819.90 (*Id.* at ¶¶ 8-9; DE-15 (Plea Agreement) at ¶ 5(e)).

Logs seized from servers involved in operating the Booters reveal that thousands of "users" ordered approximately 3,829,812 DDoS attacks in just the first

[1] One of the Booters, QuezStresser, was a free service that the co-conspirators used to introduce customers to booting and, in turn, drive traffic to their other Booters.

13 months of the 27-month long conspiracy. (PSR at ¶ 9). A summary of the Booters' users and DDoS attack order volume is set forth below:

Booter	**Total Users** (08/02/2015-08/23/2016)	**Total DDoS Attacks** (08/02/2015-08/23/2016)
Betabooter	6,685	89,965
Databooter	46,627	384,839
Decafestresser	20,138	149,356
ExoStresser	114,124	1,050,946
Instabooter	142,285	181,135
Zstress	6,004	74,996
QuezStresser	Unknown	1,898,575
Totals	**335,863**	**3,829,812**

(Ex. A (Booter Statistics)). Further, the Booters continued to launch significant volumes of DDoS attacks through late November 2017. (*See, e.g.*, DE-1 at ¶ 10). For instance, ExoStresser's website showed that it alone launched 316,664 additional attacks from around August 23, 2016 to around September 12, 2017. (*See id.*).

According to the FBI's investigation, the defendant's conduct contributed to the development, administration, and/or launch of DDoS attacks of each of the Booters. (Ex. A; DE-1 at ¶¶ 8, 34-52). For instance, the defendant registered and controlled computer infrastructure that the Booters shared to launch DDoS attacks, including servers that were rented from a hosting company and others servers that he purchased and operated from colocation facilities around the world. (PSR at ¶ 8; DE-1 at ¶¶ 37-40). Further, logs extracted from the Booters' servers revealed that the defendant administered many of the Booters, including logs showing that he

repeatedly accessed the administrative accounts of many of the Booters, and used each to order the launch of illegal DDoS attacks.[2] (*Id.*; Ex. A).

b. Harm Caused by the Booters

The DDoS attacks launched by the Booters targeted the computer systems and networks of a wide array of victims, including law enforcement, schools, military webpages, government research labs, DoD entities, corporations, and residential communities. (*See, e.g.*, PSR at ¶ 7; DE-1 ¶ 11). For instance, an examination of the Booters' order logs revealed DDoS attacks targeting hundreds of IP addresses associated with military and DoD networks, including the Army, Navy, Air Force and Pentagon. (*See* Ex. B (Defense Information Systems Agency (DISA)—Victim Impact Statement) at 2). A partial examination of URLs targeted by the Booters, moreover, showed thousands of DDoS attacks ordered against the websites of:

- More than 200 governmental entities, including the FBI and other agencies and organizations within local, federal, and foreign governments.
- More than 250 secondary and post-secondary educational institutions, including school districts in New York, Wisconsin, Florida, Pennsylvania, and Vermont; and
- Private organizations of varying sizes, including large technology companies, small and medium-sized businesses, banks and other financial institutions, and media companies.

[2] In the PSR, the defendant denied using DecafeStresser, and claimed "a more limited involvement" with Betabooter. (PSR at ¶ 7, n. 3-4). The defendant's responses are contradicted by logs that show he accessed the administrative accounts of DecafeStresser and Betabooter a minimum of 276 and 26 times, respectively, and ordered both to launch DDoS attacks (Ex. A).

(Ex. C (FBI Analysis of DDoS Attacks) - FILED SEPARATELY UNDER SEAL).[3]

The DDoS attacks launched by the Booters, in turn, disrupted the internet connections of targeted victims, rendered targeted websites slow or inaccessible, and interrupted victim operations. (PSR at ¶ 7). In a victim impact statement, the Chief of a DoD division (DISA) responsible for defending DoD against malicious cyber threats,[4] analogized the interruption caused by DDoS attacks to "protesters [who] blocked a store's entry door, preventing customers from getting in. When a server is overloaded with connections, new connections can no longer be accepted." (Ex. B at 2.)

The Booters' malicious interference with the operations of victim computer systems had real world consequences. For instance, ExoStresser advertised on its website that it alone had cost victims 109,186.4 hours of network downtime (~4,549 days). (DE-1 at ¶ 10). These were hours where victims could not access online resources, provide online services, or conduct business online.

The Booters' attacks also harmed unintended victims who shared network infrastructure with the intended targets, including the intended targets' web hosting and/or internet service providers. For example, over several days in November 2016,

---

[3] The FBI performed a partial analysis of website Uniform Resource Locators ("URLs") identified in the Booters' logs that were easily identified as government (.gov), educational institutions (.k12, .edu, "school", or "college"), or publicly known. The FBI analysis of the Booters' attack logs were provided to defense counsel on June 14, 2019, and the supporting DDoS order logs were produced via FedEx.

[4] DISA is a DoD-entity that, among other things, provides internet access points to DoD organizations and monitors and analyzes DoD internet traffic to defend the DoD information network from malicious cyber threats. (*See* Ex. C at 1).

the Betabooter service launched at least four DDoS attacks against the Franklin Regional School District in the Pittsburgh, Pennsylvania area that not only disrupted its computer systems, but affected the computer systems of more than 17 organizations that shared the same infrastructure in Westmoreland County. Victims of the attack included (i) other school districts, (ii) the Westmoreland County government, (iii) the county's three career technology centers, and (iv) The Catholic Diocese of Greensburg, Pennsylvania. (PSR at ¶ 7). The attacks caused affected school districts to lose valuable educational time by rendering inaccessible online educational resources and e-mail accounts used by teachers and administrators. In a victim impact statement, the Deputy Director of Information Security for Westmoreland County, further explained how the attacks brought parts of the county government to a "halt" during the outages:

> Any internal department that uses the internet for communications to their core application (web-based) was brought to a halt. Those include, but are not limited to, the Children's Bureau, Veteran's Affairs, Courts, Juvenile Probation/Detention, Elections Bureau, County Manor (Nursing Home), and access to any state issued licenses offered internally . . . . This caused not only a hiatus in work for the department, but also a need to turn away members of the public for services that could not be offered during the attack.

(Ex. D [Westmoreland County Gov't—Victim Impact Statement] at 1). The Betabooter attacks also disrupted certain paid services that the County offered, such as online deeds, tax documents, and mapping data. (*Id.*) In addition "[t]he outages required the county to give partial re-imbursements to clients for the month of November[] 2016, and caused a great inconvenience to anyone who relies on this data for their own business, employment or well-being." (*Id.*)

To defend against the Booters' attacks, victims were also forced to expend valuable time and resources strengthening their cyber defenses. As the Chief of DISA Mission Division detailed:

> The attacks launched by Mr. Usatyuk were serious threats DISA had to defend against. Our efforts to deal with his crimes have consumed DoD resources that would have been better used to defend against our peer and non-peer competitors.

(Ex. B at 2). The stakes of DISA's work were high; as even a single "successful attack on our systems could result in mission failure and cost the lives of our service members," as well as degrade "our leaders' ability to maintain awareness of current events and successfully control our own forces . . . ." (*Id.* at 1). The Booters also increased the cost of doing business online. For instance, in or around July 2016, ExoStresser was one of a number of booters that cybercriminals used to repeatedly attack servers of a video game manufacturer that hosted a popular multi-player videogame. (DE-1 at ¶ 12). The attacks contributed to the video game manufacturer suffering an estimated $164,000 loss from defending and remediating the harm caused by DDoS attacks against the game. (*Id.*)

To facilitate the illegal DDoS attacks, the Defendant also illegally exploited third-party computers to reflect and amplify the Booters' unauthorized web traffic, including computer systems within the District. (DE-1 at ¶¶ 14, 43).

c. The Defendant Used Sophisticated Means to Evade Detection

The defendant deployed a number of sophisticated techniques and fake online personas to evade detection during the co-conspirators' 27-month conspiracy. As an initial matter, the Booters typically launched DDoS attacks using a technique known

as IP spoofing and DDoS amplification that made it extremely difficult to trace the attacks back to the co-conspirators' computer infrastructure. Notably, by leveraging unconsenting "amplification servers" as intermediaries for reflecting and amplifying traffic towards a targeted victim computer system, the defendant ensured that victims of the Booters' DDoS attacks would mistakenly think they were attacked by innocent, third-party computers that reflected traffic and fail to recognize the co-conspirators' role when reporting attacks to law enforcement.

To further conceal the co-conspirators' identity and criminal activity, the defendant created accounts with DDoS mitigation services that obscured the Booters' true IP addresses, and used a number of aliases and online monikers to administer the Booters, including "Andrew Quez," "Andy Quez," "Brian Martinez," and "GiftedPVP," among others. (*See* DE-1 at ¶¶ 1, 31, 34, 36; Ex. A). The co-conspirators also circumvented payment processor controls against malicious online activity by channeling their customers' fees through a vast network of fraudulent payment processing accounts created with false information, as well as converting the conspiracy's gains to Bitcoin at a rate of 15 or more percent. (*See* DE-1 at ¶¶ 31, 54, 58; Ex. E (Excerpts of Def.'s Messages) at 1). Indeed, in 2016, the co-conspirators' system of fraudulent payment processing accounts had become so involved that they discussed plans to automate the process of cashing out of money. (Ex. E at 1).

III. Defendant's Plea Agreement and Applicable Guidelines Range

On February 27, 2019, pursuant to a written plea agreement with the government, the defendant waived indictment and entered a guilty plea to a one

count Criminal Information that charged him with conspiracy to cause damage to protected computers under 18 U.S.C. § 1030(a)(5)(A), in violation of 18 U.S.C. § 371. (*See* DE-1 (Criminal Information), 14 (Waiver of Indictment), 15 (Plea Agreement)). As part of the plea agreement, the parties agreed to a number of sentencing factors that resulted in a recommended offense level of 25, including a stipulation that loss could not be reasonably determined here and that an upward adjustment of 14 levels was warranted under USSG §2Bl.1(b)(1)(H) based on the co-conspirators' gain of between $550,000 and $1,500,000. (DE-15 at ¶ 5(a)).

The USPO published a final PSR on June 12, 2019 (DE-22) that mirrored the parties' stipulations and likewise recommended an offense level of 25, and a guideline imprisonment range of 57 to 60 months. (PSR at ¶¶ 33-47). As reflected in the PSR and the recommendation in the plea agreement, defendant's total offense level for his crime is calculated as follows:

Guideline	**Offense Level**
Base Offense Level (Section §§2X1.1(a) and 2B1.1(a)(2))	6
Loss / Gain amount exceeds $550,000, but was less than $1,500,000. (Section 2B1.1(b)(1)(H))	+14
The offense involved 10 or more victims (Section 2B1.1(b)(2)(A)(i))	+2
The offense involved sophisticated means. (Section §2B1.1(b)(10)(C))	+2
Defendant was convicted of an offense under 18 U.S.C. § 1030(a)(5)(A). (Section 2B1.1(b)(19)(A)(ii))	+4
Acceptance of responsibility (Section 3E1.1(a)-(b))	-3
Total Offense Level	**25**

(PSR at ¶¶ 33-47). Given the defendant's timely acceptance of responsibility, the government moves the Court for a one-level reduction under U.S.S.G. § 3E1.1(b), as the USPO has appropriately included in the above calculations. (*Id*. at ¶¶ 44-45).

With a criminal history category of I and an adjusted offense level of 25, the defendant's advisory guidelines imprisonment range is 57 to 60 months.

IV. The Appropriate Sentence In Light of 18 U.S.C. § 3553(a)

To determine the appropriate sentence for defendant's offense, the Court must consider both the Sentencing Guidelines and the sentencing factors in 18 U.S.C. § 3553(a). Although the Sentencing Guidelines are advisory, district courts are required to "consult those Guidelines and take them into account when sentencing." *United States v. Booker*, 543 U.S. 220, 264 (2005). Under the required procedure, a "district court should begin all sentencing proceedings by correctly calculating the applicable Guidelines range," which "should be the starting point for the initial benchmark." *Gall v. United States*, 552 U.S. 38, 49 (2007).

Section 3553(a) requires the Court to then analyze a number of factors, including "the nature and circumstances of the offense"; "the history and characteristics of the defendant"; "the need for the sentence imposed to reflect the seriousness of the offense, to promote respect for the law, and to provide just punishment for the offense"; the need "to afford adequate deterrence"; and "the need to protect the public from further crimes of the defendant." 18 U.S.C. § 3553(a); *see Gall*, 552 U.S. at 50 n.6; *United States v. Hughes*, 401 F.3d 540, 546 (4th Cir. 2005).

Here, all of these Section 3553(a) factors weigh in favor of a substantial prison sentence. The Government therefore submits that a sentence of 57 months at the low-end of the guidelines would be sufficient and not greater than necessary to reflect the extraordinary seriousness of the defendant's conduct, promote respect for the law, provide just punishment for the offense, and deter both the defendant and others.

A. Nature and Circumstances of the Offense

The known scope, breadth, and duration of the defendant's scheme to launch millions of cyber-attacks warrants a substantial period of incarceration that adequately accounts for the widespread harm the defendant caused and intended to cause to victim computer systems, including the many systems that were foreseeably impacted by the Booters. Indeed, as detailed above, the defendant's conduct over a 27-month period paved the way for at least 3,829,812 DDoS attacks that, among other things, interrupted school and governmental services, knocked targeted computer systems offline, raised the price of doing business online for private businesses and entities, and posed "serious threats" that unnecessarily consumed valuable DoD resources. (PSR at ¶¶ 7-9; Exhs. B, D; DE-1 at ¶¶ 10-14). The Booters were so potent that cyber criminals continued to flock to them over a 27-month period, and paid over a half million dollars to continue launching damaging DDoS attacks. (*See id*.).

While these metrics alone underscore the seriousness of the defendant's crimes, it is important to recognize that they likely only capture a subset of the real world harm caused by the co-conspirators' conduct. As detailed above, the Booters used a technique known as IP spoofing and DDoS amplification to conceal the role of

the co-conspirators' infrastructure in DDoS attacks, and thwart the FBI's methodical and painstaking efforts to identify the perpetrators. In fact, when a third-party notified the defendant that an illegal DDoS attack had been traced to ExoStresser's servers, the defendant himself boasted that "[y]ou also didn't 'trace' anything back to us, if you understood how DrDoS amplification works ***you'd know it's impossible to be traced*** . . . ." (Ex. E at 1 (Emphasis Added)).

In addition, the estimates in the PSR are based on the volume of DDoS attacks ordered during the first 13 months of the conspiracy. The Booters' logs for the last 14 months of the conspiracy could not be recovered. Although the precise timing of destruction is not known, an electronic chat between the defendant and Co-conspirator A reveals the co-conspirators discussed the need to destroy DDoS attack logs on or around November 8, 2016. (Ex. E at 2; DE-1 ¶ 47). Notably, in response to the arrest of an administrator of another DDoS-for-hire service, the defendant described plans to remove his personal logs to get rid of evidence, and warned Co-Conspirator A to do the same: "If they [law enforcement] get the DB [database] and see your name in the log fields they won't care about much else." (*Id*.). The defendant further cautioned that "[p]olice were able to nail [the arrested administrator] thanks in part to his keeping of DDoS attack logs." (*Id*.)

As these chats underscore, a significant sentence is also warranted here because the defendant unquestionably knew that his conduct was illegal throughout the 27-month conspiracy. Indeed, more than a year before unveiling the Booters, the FBI ***personally notified*** the defendant that it was illegal to launch DDoS attacks

during two interviews concerning his role in an earlier large-scale DDoS attack that took down an influential technology website named KrebsonSecurity. (PSR at ¶ 6). In successive interviews in March 2014, the defendant admitted to participating in the attack, advertising and selling DDoS services online, receiving payments via PayPal and Bitcoin, and leasing third-party servers to facilitate attacks. (*Id.*) At the time, the defendant assured the FBI investigators that he would stop executing DDoS attacks and avoided prosecution as an adult (he was only 15 at the time). (*Id.*)

The defendant's promises proved hollow. Within two years of the FBI's visits to his home, the defendant not only elected to resume launching DDoS attacks; but dramatically escalated the seriousness and scope of his criminal conduct by unveiling services that could help thousands of other cyber criminals do the same. The defendant's willful disregard for the FBI's warnings and unambiguous knowledge of how the Booters were used in crime is evidenced by the defendant's sophisticated efforts to evade law enforcement detections, the defendant's own words and repeated notifications that he received from third-parties about the Booters' illegal activities.

For instance, after a potential customer asked about using ExoStresser for a legitimate purpose, the co-conspirators exchanged electronic chats on or around April 12, 2016, in which they joked about their potential criminal exposure:

> *Defendant*: for when raid comes im [expletive] save this ticket.
>
> *Co-Conspirator A*: Users is a bit of a stretch.
>
> *Defendant*: Take that FBI. legitimate stress test users we have holy [expletive]

(Ex. E at 2). Further, the defendant repeatedly attempted to eliminate the competition posed by similar DDoS-for-hire services by perversely using his knowledge of the applicable law to report their illegal activity. (*Id.* at 2). For instance, on December 23, 2014, the defendant detailed to a provider:

> This website is a 'booter,' or a DDoS for hire tool responsible for sending hundreds of ***illegal distributed denial of service attacks*** on a daily basis. Please not (sic) that you yourself will not see any DDoS traffic originating from this website, this website uses offshore servers . . . to send the actual DDoS attacks, however ***the website is a tool that makes these offshore servers launch the actual DDoS, thus still violating the law***.

(Ex. E at 3 (Emphasis added)).

As the defendant tried to win customers by eliminating DDoS-for-hire competitors, web hosting providers and other third-parties were simultaneously sending the defendant notifications that his Booters were likewise launching illegal DDoS attacks. (*Id.* at 3). The Booters' violations of third-party policies were sometimes so egregious that the defendant's accounts were suspended or discontinued for terms of service violations. (*See, e.g.*, *id.*). However, rather than stop the illegal activities, the defendant kept the Booters operational by changing service providers, obfuscating his customers' conduct, and eventually transitioning to servers that he controlled and operated from datacenters in Chicago, Illinois and Bucharest, Romania under the front of an entity named "OkServers LLC." (*See, e.g.*, PSR at ¶ 8).

Accordingly, as a principal architect of the Booters, the defendant's willful role in facilitating millions of illegal DDoS attacks warrants a significant sentence.

B. The History and Characteristics of the Defendant

The defendant's crimes here were not some momentary lapses of judgment. The defendant has engaged in illegal online activity since as early as 2014. (*See* PSR at ¶ 6). Even after twice speaking with the FBI in 2014, the defendant made countless choices over the 27-month period to create a sophisticated criminal enterprise dedicated to committing cyber-crime on a massive scale. (*See id.* at ¶¶ 6-8). The defendant knew each of his choices were illegal, including obscuring the Booters' criminal infrastructure; registering accounts under aliases and fictitious monikers; guiding cyber criminals on how to launch illegal DDoS attacks; deceiving payment processing and hosting providers; channeling gains through cryptocurrency; and deleting logs and other records to conceal his crimes. (*See, e.g.*, *id.*)

Further, even after entering a guilty plea in this case, the Government received information from counsel for the town Lauderdale-by-the-Sea, Florida concerning a troubling public records request that was submitted by the defendant on or around July 21, 2019 seeking "every single email address" that the municipality had on record. (Ex. F (Defendant's Public Records Request)). Despite multiple requests, the defendant has yet to provide a legitimate, non-malicious explanation for his, at best, highly-questionable and improper phishing for personal emails.

Accordingly, although the defendant has no formal criminal history, the government believes the defendant's extensive track record of willful defiance of the law and malicious online activity suggests likelihood of recidivism if left undeterred by a significant term of incarceration. The risk of recidivism is particularly acute here

given the defendant's repeated decisions to choose cyber-crime over legitimate pursuits despite having opportunities that were never within the reach of many offenders who come before this Court, including a stable upbringing, financial support from his parents, good educational opportunities, and impressive technical skills.[5]

The defendant's guideline calculation of 57 to 60 months does already credit the defendant's acceptance of responsibility with a 3-point reduction in his guidelines under Section 3E1.1. Further, in recognition that the defendant is 21 years old, and was a minor for the first 8 (of 27) months of the charged conspiracy, the government has proposed a sentence of 57 months that is at the low-end of the guidelines.

However, in view of the seriousness of the defendant's sustained and willful conduct—the clear majority of which occurred after turning 18, the defendant's history and characteristics do not merit any further variance/departure and support a significant sentence.

C. The Need for the Sentence Imposed to Reflect the Seriousness of the Offense, To Promote Respect for the Law, Provide Just Punishment, and Afford Adequate Deterrence to Criminal Conduct

A sentence within the Guideline Range would address the seriousness of the defendant's crimes and provide just punishment. It would also promote respect for the law and provide individualize deterrence. As detailed above, in 2014, the then-15 year old defendant evaded prosecution for his role in a significant DDoS. At the time, the defendant had an opportunity to stop his wrongful and illegal conduct and choose to

[5] "Criminals who have the education and training that enables people to make a decent living without resorting to a crime are more rather than less culpable than their desperately poor and deprived brethren in crime." *United States v. Stefonek*, 179 F.3d 1030, 1038 (7th Cir. 1999).

apply his talents towards other legitimate pursuits. He did not. Instead, the defendant responded to the 2014 incident by escalating both his criminal conduct and efforts to evade detection. Indeed, as detailed above, the defendant was acutely aware and openly dismissive of the FBI's efforts to combat the precise conduct that he was perpetrating. A significant sentence is needed here to affirm respect for laws barring illegal DDoS attacks, and deter the defendant from further recidivism.

The court should further impose a significant sentence to generally deter other cyber criminals who may seek to launch similarly serious DDoS attacks. *See, e.g.*, *Ferguson v. United States,* 623 F.3d 627, 632 (8th Cir. 2010) (quoting *United States v. Medearis*, 451 F.3d 918, 920 (8th Cir. 2006)) ("Congress specifically made general deterrence an appropriate consideration . . . , and we have described it as 'one of the key purposes of sentencing.'"). In fact, a number of the DDoS attack types used by the Booters have posed such a systemic cyber threat that the United States Computer Emergency Readiness Team (US-CERT) within the Department of Homeland Security has issued public alerts about them. (Ex. G (Alert (TA14-017A)-UDP Based Amplification Attacks, Alert (TA13-088A)-DNS Amplification Attacks), Alert (TA14-013A)-NTP Amplification Attacks).

As this case illustrates, cyber criminals exploit the invisibility afforded by the Internet, cryptocurrency, and other masking tools to evade detection for many years. Indeed, many internet crimes go unsolved and unpunished due to the tremendous resources it takes for law enforcement to pierce through a cyber criminal's cloak of anonymity. Accordingly, when someone like the defendant is identified and

apprehended, a substantial sentence is needed to provide a message of deterrence to other would-be cyber criminals.

D. A Significant Sentence is Consistent With Sentences In Other Cases

Recent prosecutions of mere *customers* of booting services and individuals who launched isolated DDoS attacks underscores the reasonableness of imposing a substantial sentence. For instance, in 2017, a district court in Minnesota imposed a 5-year sentence for a count of conspiracy to cause damage to protected computers in a case involving a defendant who launched DDoS attacks against dozens of victims using illegal booter services similar to the ones offered by the defendant in this case.[6] *See* Amended Sentencing Judgment, DE 133, *United States v. Gammell*, No. 0:17-cr-00134-WMW-DTS (D. Minn. July 31, 2018), *aff'd,* No. 18-2692 (8th Cir. 2019 Aug. 9, 2019). The sentence was affirmed by the 8th Circuit Court of Appeals. *Id*.

Similarly, earlier this year, a federal judge in San Diego, California sentenced a 23-year old man to a guideline sentence of 27 months[7] in prison for launching a number of DDoS attacks against the servers of corporate victims over a three week period. Judgment, DE 28, *United States v. Thompson*, No. 18-CR-4775 (S.D. Cal. July 2, 2019). The sentence in that case was predicated on a loss figure of less than $95K, and involved a defendant who used tools developed by others to launch DDoS attacks.

---

[6] Although the defendant in that case was also sentenced to 180 months on felon-in-possession counts that ran concurrently, the Court's order was clear that a 60 month sentence was imposed for the count of conspiracy to cause damage to protected computers. *See, e.g.*, *id*.

[7] Because the defendant had an offense level of 17 and criminal history of II, the defendant's guideline range was 27-33 months.

The scale, scope, and duration of the defendant's criminal conduct are quantitatively and qualitatively more serious than the conduct pleaded to by Gammell and Thompson. Accordingly, the Government respectfully submits that the multi-year sentences imposed in those cases underscores the reasonableness of the Court imposing a substantial term of imprisonment here.

V. Conclusion

For the reasons set forth above, the government respectfully requests that the Court impose a term of incarceration of 57 months. The government submits that this sentence is sufficient, but not greater than necessary, to serve the legitimate purposes of sentencing set forth in 18 U.S.C. § 3553(a).

Respectfully submitted this 15th day of August, 2019.

By: /s/ *Aarash A. Haghighat*
AARASH A. HAGHIGHAT
Trial Attorney
U.S. Department of Justice
1301 New York Ave., NW
Suite 600
Washington, DC 20005
Telephone: 202-616-2929
Email: Aarash.haghighat@usdoj.gov

ADAM F. HULBIG
Assistant United States Attorney
Criminal Division
310 New Bern Avenue, Suite 800
Raleigh, North Carolina 27601
Telephone: (919) 856-4530
Fax: (919) 856-4487
E-mail: adam.hulbig@usdoj.gov

CERTIFICATE OF SERVICE

I hereby certify that on this 15th day of August, 2019, I served a copy of the foregoing Government's Sentencing Memorandum upon the defendant in this action by electronically filing the same with the Clerk of Court using the CM/ECF system, which will send notification of such filing to the defendant's counsel of record as follows:

Katherine E. Shea
Federal Public Defender
Email: kat_shea@fd.org

By: /s/ *Aarash A. Haghighat*
AARASH A. HAGHIGHAT
Trial Attorney
U.S. Department of Justice
1301 New York Ave., NW
Suite 600
Washington, DC 20005
Telephone: 202-616-2929
Email: Aarash.haghighat@usdoj.gov